Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра Информационных технологий и систем безопасности

Рабочая программа по дисциплине

ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основная профессиональная образовательная программа
высшего образования программы специалитета по специальности

10.05.02 «Информационная безопасность телекоммуникационных систем»

Специализация:
Разработка защищенных телекоммуникационных систем

Квалификация:
Специалист

Форма обучения
Очная

Согласовано
Руководитель ОПОП
«Информационная безопасность телекоммуникационных систем»

_____ Бурлов В.Г.

Утверждаю
Председатель УМС _____И.И. Палкин

Рекомендована решением
Учебно-методического совета
18 мая 2018 г., протокол № 4

Рассмотрена и утверждена на заседании кафедры
17 мая 2018 г., протокол № 5
Зав. кафедрой _____ Бурлов В.Г.

Авторы-разработчики:
_____ Ананченко И.В.

Санкт-Петербург 2018

1. Цели освоения дисциплины

Цели освоения дисциплины «Программно-аппаратные средства обеспечения ИБ» является формирование у студентов знаний и умений по защите компьютерной информации, обрабатываемой и хранимой в современных автоматизированных системах (АС), от неправомерного доступа, перехвата и разрушающего программного воздействия, на основе применения современных программно-аппаратных средств.

Приобретенные знания позволят студентам выполнять задачи по проектированию и разработке программно-аппаратных средств защиты информации, правильно ориентироваться в многообразии выпускаемых и предлагаемых средств информационной защиты, обоснованно выбирать те из них, которые отвечают требованиям, предъявляемым к защите информации в конкретной автоматизированной системе, а также оценивать эффективность безопасности информационных технологий.

Задачи получение учащимися базовых знаний о процессе и методах использования программно-аппаратных средств для обеспечения информационной безопасности.

2. Место дисциплины в структуре ОП

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» для направления подготовки 10.05.02 – информационная безопасность телекоммуникационных систем относиться к дисциплинам базовой части Блока1 Дисциплины (Модули) (Б1.Б.11).

Для освоения данной дисциплины, необходимо обладать базовыми знаниями (общее среднее образование), а также освоить учебный материал предшествующих дисциплин:
«Информатика и программирование», «Теория вероятностей и математическая статистика», «Дискретная математика», «Основы информационной безопасности», «Телекоммуникационные системы», «Сети и системы передачи информации», «Моделирование систем и сетей телекоммуникаций».

Параллельно с дисциплиной «Программно-аппаратные средства обеспечения ИБ» изучаются дисциплины: «Теория принятия решения в условиях информационных конфликтов», «Проектирования защищенных телекоммуникационных систем», «Сетевое администрирование», «Информационная безопасность ТКС», «Разработка защищенных ТКС».

Знания и практики, полученные обучаемыми по дисциплине «Программно- аппаратные средства обеспечения ИБ», непосредственно используются при написании выпускной работы студента и в практической профессиональной деятельности, связанной с защитой информации от утечки по техническим каналам.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код компетенции	Компетенция
ОПК-5	способностью применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач
ПК-14	способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем
ПСК-7.5	способностью обеспечивать защиту программных средств защищенных телекоммуникационных систем;

В результате освоения компетенций в рамках дисциплины обучающийся должен:

Код компетенции	Результаты обучения
ОПК-5	– Знать: – программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах и СУБД; – классификацию и общую характеристику программно-аппаратных средств защиты информации; – общие принципы построения программно-алгоритмических средств защиты информации в сложных клиентских приложениях; Уметь: – правильно применять средства антивирусной защиты отечественных и зарубежных производителей; – использовать современные методы и алгоритмы защиты от вредоносных программ; – правильно использовать защитные механизмы, внедренные на прикладном программном уровне; Владеть: – навыками защиты от изменения и контроля целостности программ;
ПК-14	Знать: – основные средства защиты компьютерной информации, компьютерных систем и машинных носителей информации от непосредственного доступа; – методы и средства защиты компьютерной информации в устройствах долговременной памяти; – методы защиты компьютерной информации средствами СУБД; – основные принципы администрирования защищенных автоматизированных систем; – особенности реализации методов защиты информации программно-аппаратными средствами; Уметь: – обеспечивать защиту от разрушающих программных воздействий; – конфигурировать и настраивать работоспособность вычислительных систем;

	– применять наиболее эффективные методы и средства программно-аппаратной защиты информации; – выполнять функции администратора безопасности защищенных компьютерных систем; Владеть: – современными средствами защиты АС от несанкционированного доступа; – средствами администрирования программно-аппаратных комплексов защиты информации от несанкционированного доступа; – средствами администрирования комплексов криптографической защиты информации
ПСК-7.5	Знать: – программно-алгоритмические методы защиты компьютерной информации; – основные средства защиты компьютерной информации, компьютерных систем и машинных носителей информации от непосредственного доступа; – принципы комплексирования средств и методов защиты компьютерной информации; Уметь: – анализировать и оценивать угрозы информационной безопасности, осуществлять рациональный выбор средств и методов защиты информации объектов информатизации; – выполнять настройку защитных механизмов программно-аппаратных средств; – настраивать политику безопасности средствами программно-аппаратных комплексов защиты информации; – применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных систем; Владеть: – методами и средствами обеспечения информационной безопасности; – методами расчета и инструментального контроля показателей защиты информации;

Основные признаки формируемых компетенций в результате освоения дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» сведены в таблице.

Уровень освоения компетенции	**Результат обучения**	**Результат обучения**	**Результат обучения**
	ОПК-5: Знать, уметь, владеть	ПК-14: Знать, уметь, владеть	ПСК-7.5: Знать, уметь, владеть
минимальный	Способен дать собственную критическую оценку изучаемого материала	Способен дать собственную критическую оценку изучаемого материала	Способен дать собственную критическую оценку изучаемого материала
	Может соотнести основные идеи с современными проблемами	Может соотнести основные идеи с современными проблемами	Может соотнести основные идеи с современными проблемами
	Способен выделить характерный авторский подход	Способен выделить характерный авторский подход	Способен выделить характерный авторский подход
базовый	Способен сравнивать концепции, аргументированно излагает материал	Способен сравнивать концепции, аргументированно излагает материал	Способен сравнивать концепции, аргументированно излагает материал
	Аргументированно проводит	Аргументированно проводит	Аргументированно проводит

	сравнение концепций по заданной проблематике	сравнение концепций по заданной проблематике	сравнение концепций по заданной проблематике
	Способен выделить специфику концепций в заданной проблемной области	Способен выделить специфику концепций в заданной проблемной области	Способен выделить специфику концепций в заданной проблемной области
продвинутый	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области
	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области
	Может дать критический анализ современным проблемам в заданной области анализа	Может дать критический анализ современным проблемам в заданной области анализа	Может дать критический анализ современным проблемам в заданной области анализа

Соответствие уровней освоения компетенции планируемым результатам обучения и критериям их оценивания

Этап (уровень) освоения компетенции	Основные признаки проявленности компетенции (дескрипторное описание уровня)				
	1.	2.	3.	4.	5.
минимальный	не владеет	слабо ориентируется в терминологии и содержании	Способен выделить основные идеи текста, работает с критической литературой	Владеет основными навыками работы с источниками и критической литературой	Способен дать собственную критическую оценку изучаемого материала
	не умеет	не выделяет основные идеи	Способен показать основную идею в развитии	Способен представить ключевую проблему в ее связи с другими процессами	Может соотнести основные идеи с современными проблемами
	не знает	допускает грубые ошибки	Знает основные рабочие категории, однако не ориентируется в их специфике	Понимает специфику основных рабочих категорий	Способен выделить характерный авторский подход
базовый	не владеет	плохо ориентируется в терминологии и содержании	Владеет приемами поиска и систематизации, но не способен свободно изложить материал	Свободно излагает материал, однако не демонстрирует навыков сравнения основных идей и концепций	Способен сравнивать концепции, аргументированно излагает материал
	не умеет	выделяет основные идеи, но не видит проблем	Выделяет конкретную проблему, однако излишне упрощает ее	Способен выделить и сравнить концепции, но испытывает сложности с их практической привязкой	Аргументированно проводит сравнение концепций по заданной проблематике
	не знает	допускает много ошибок	Может изложить основные рабочие категории	Знает основные отличия концепций в заданной проблемной области	Способен выделить специфику концепций в заданной проблемной области
продвинутый	не владеет	ориентируется в терминологии и содержании	В общих чертах понимает основную идею, однако плохо связывает ее с существующей проблематикой	Видит источники современных проблем в заданной области анализа, владеет подходами к их решению	Способен грамотно обосновать собственную позицию относительно решения современных проблем в заданной области
	не умеет	выделяет основные идеи, но не видит их в развитии	Может понять практическое назначение основной идеи, но затрудняется выявить ее основания	Выявляет основания заданной области анализа, понимает ее практическую ценность, однако испытывает затруднения в описании сложных объектов анализа	Свободно ориентируется в заданной области анализа. Понимает ее основания и умеет выделить практическое значение заданной области
	не знает	допускает ошибки при выделении рабочей области анализа	Способен изложить основное содержание современных научных идей в рабочей области анализа	Знает основное содержание современных научных идей в рабочей области анализа, способен их сопоставить	Может дать критический анализ современным проблемам в заданной области анализа

4. Структура и содержание дисциплины

Общая трудоемкость (объем) дисциплины (модуля) составляет 4 зачетные единицы, 144 академических часа.

Объем дисциплины по видам учебных занятий в академических часах)

Объём дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоёмкость дисциплины	**144**
Контактная работа обучающихся с преподавателям (по видам аудиторных учебных занятий) – всего:	**72**
в том числе:	
лекции	**36**
лабораторные занятия	**36**
Самостоятельная работа	**72**
В том числе:	
Курсовая работа	+
Вид промежуточной аттестации	**Зачёт с оценкой**
Всего:	**144**

4.1. Структура дисциплины

№ п/п	**Раздел и тема дисциплины**	**Семестр**	**Виды учебной работы, в т.ч. самостоятельная работа студентов, час.**			**Формы текущего контроля успеваемости**	**Занятия в активной и интерактивной форме, час.**	**Формируемые компетенции**
			Лекции	**Лабораторные**	**Самост. работа**			
1	Введение. Предмет курса и его задачи.	**9**	5	5	20	Устный опрос по изучаемой теме	10/4	ОПК-5, ПК-14
2	Идентификация пользователей КС – субъектов доступа к данным	**9**	2	2	2	Устный опрос по изучаемой теме	4	ПК-14, ОПК-5
3	Средства и методы ограничения доступа к файлам	**9**	2	2	2	Устный опрос по изучаемой теме	4	ПК-14
4	Особенности защиты данных от изменения. Программно-аппаратные средства шифрования	**9**	5	5	14	Устный опрос по изучаемой теме	10/4	ПК-14, ПСК-7.5

5	Построение программно-аппаратных комплексов шифрования	**9**	2	2	2	Устный опрос по изучаемой теме	4	ОПК-5, ПК-14, ПСК-7.5
6	Методы и средства ограничения доступа к компонентам ЭВМ	**9**	6	6	15	Устный опрос по изучаемой теме	12/4	ПК-14
7	Особенности защиты данных от изменения. Программно-аппаратные средства шифрования	**9**	2	2	2	Устный опрос по изучаемой теме	4	ПСК-7.5, ОПК-5
8	Защита программ от изучения. Аппаратный ключ с точки зрения электроники.	**9**	6	6	15	Устный опрос по изучаемой теме	12/6	ПСК-7.5, ПК-14
9	Защита от разрушающих программных воздействий.	**9**	6	6	10	Устный опрос по изучаемой теме	12/4	ПСК-7.5, ПК-14
	ИТОГО		36	36	72		72/18	

4.2. Содержание разделов дисциплины

4.2.1. Введение

Предмет курса и его задачи. Электронный документ (ЭД). Виды информации в КС. Информационные потоки в КС. Понятие ЭД. Типы ЭД. Понятие исполняемого модуля. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа. Понятие несанкционированного доступа (НСД). Классы и виды НСД. Несанкционированное копирование программ как особый вид НСД. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).

4.2.2. Идентификация пользователей КС – субъектов доступа к данным

Политика безопасности в компьютерных системах. Оценка защищенности. Способы защиты конфиденциальности, целостности и доступности в КС. Понятие идентификации пользователя. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация. Аутентификация. Понятие идентифицирующей информации. Способы хранения идентифицирующей информации. Связь с ключевыми системами.

4.2.3 Средства и методы ограничения доступа к файлам

Основные подходы к защите данных от НСД. Шифрование. Контроль

доступа. Разграничение доступа. Оценка надежности систем ограничения доступа. Иерархический доступ к файлам. Понятие атрибутов доступа. Организация доступа к файлам различных ОС. Защита сетевого файлового ресурса на примерах организации доступа в различных ОС. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД. Доступ данных со стороны процесса. Понятие доступа к данным со стороны процесса. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.

4.2.4 Особенности защиты данных от изменения. Программно-аппаратные средства шифрования

Защита массивов информации от изменения (имитозащита). Криптографическая постановка защиты от изменения данных. Подходы к решению задачи защиты данных от изменения. Защита от разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.

4.2.5 Построение программно-аппаратных комплексов шифрования

Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носителя алгоритма шифрования. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа. Необходимые и достаточные функции аппаратного средства криптозащиты. Проектирование модулей криптопреобразований на основе сигнальных процессов.

4.2.6 Методы и средства ограничения доступа к компонентам ЭВМ

Компоненты ПЭВМ. Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ. Процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей. Механизмы расширения BIOS. Преимущества и недостатки программных и аппаратных средств. Проблемы использования расширенной BIOS: эмуляция файловой системы до загрузки ОС и т.д.

4.2.7 Проблема защиты отчуждаемых компонентов ПЭВМ. Привязка ПО к внешним (добавляемым) аппаратным элементам

Способы защиты информации на съемных дисках. Организация прозрачного режима шифрования. Надежность средств защиты компонент. Понятие временной и гарантированной надежности. Защита программ от несанкционированного копирования. Юридические аспекты несанкционированного копирования программ. Обще понятие защиты от копирования. Разновидности задач защиты от копирования. Подходы к задаче защиты от копирования.

Привязка к портовым ключам. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев». Хранение ключей информации. Пароли и ключи. Секретная информация,

используемая для контроля доступа: ключи и пароли. Злоумышленник и ключи. Классификация средств хранения ключей и идентифицирующей информации. Организация хранения ключей (с примерами реализации). Магнитные диски прямого доступа. Магнитные и интеллектуальные карты. Средство TouchMemory. Типовые решения в организации типовых систем. Открытое распределение ключей. Метод управляемых векторов.

428. Защита программ от изучения. Аппаратный ключ с точки зрения электроники.

Изучение и обратное проектирование ПО. Понятие изучения и обратного проектирования ПО. Цели и задачи изучения работы ПО. Способы изучения ПО: статистическое и динамическое изучение. Роль программной и аппаратной среды. Временная надежность (невозможность обеспечения гарантированной надежности). Задачи защиты от изучения и способы их решения. Динамическое преобразование кода.

Защита от отладки. Итеративный программный замок. Принцип ловушек и избыточного кода. Защита от дизассемблирования. Принцип внешней загрузки файлов. Динамическая модификация программы. Защита от трассировки по прерываниям. Способы ассоциирования защиты и программного обеспечения. Оценка надежности защиты от отладки. Ключи на базе перепрограммируемой постоянной памяти. Ключи на базе заказных чипов. Примеры реализации ключей (HASP, eToken, ruToken, Guardant). Ключи на базе микропроцессоров.

429. Защита от разрушающих программных воздействий.

Модели взаимодействия прикладной программы и программы злоумышленника, компьютерные вирусы как особый класс РПВ, активная и пассивная защита, необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды, защита программ от изменения и контроль целостности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения ИБ. Основные категории требований к программной и программно- аппаратной реализации средств обеспечения информационной безопасности; программно- аппаратные средства обеспечения информационной безопасности в типовых ОС, СУБД, вычислительных сетях.

4.3. Семинарские, практические, лабораторные занятия, их содержание

№ п/п	№ раздела дисциплины	Тема занятия	Форма проведения	Формируемые компетенции
1	1	Администрирование системы защиты информации ViPNet. Состав программного комплекса ViPNet (Administrator, Client, Coordinator).	Практическая	ПСК-7.5, ПК-14

2	2	Администрирование системы защиты информации ViPNet. Развертывание защищенной VPN сети.	Практическая	ПК-14, ОПК-5
3	3	Администрирование системы защиты информации ViPNet. Программно-аппаратные комплексы ViPNet.	Практическая	ОПК-5, ПК-14
4	4	Администрирование системы защиты информации ViPNet. Межсетевое экранирование.	Практическая	ПК-14, ОПК-5
5	5	Администрирование системы защиты информации ViPNet. Типовые схемы применения ПО ViPNet.	Практическая	ОПК-5, ПК-14, ПСК-7.5
6	6	Аппаратные ключи защиты серии Guardant.	Практическая	ПСК-7.5, ПК-14
7	7	Аппаратные ключи защиты серии eToken.	Практическая	ПК-14, ОПК-5
8	8	Аппаратные ключи защиты серии ruToken.	Практическая	ПСК-7.5, ПК-14
9	9	Аппаратные ключи защиты серии HASP4. Аппаратные ключи защиты серии HASP HL.	Практическая	ПК-14, ПСК-7.5

5. Учебно-методическое обеспечение самостоятельной работы студент и оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

5.1. Текущий контроль

Текущий контроль производится путем тестирования и проверки контрольных работ.

5.2. Методические указания по организации самостоятельной работы

Во время самостоятельной работы студенты знакомятся с проведением расчетов проектируемых параметров сети. В перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине «Программно-аппаратные средства обеспечения ИБ» входит:

1. Методические указания по выполнению практических работ.
2. Дополнительный лекционный материал

Контроль исполнения самостоятельных работ осуществляется преподавателем с участием студентов в форме обсуждения выполненных заданий и работ.

Источники для самостоятельной подготовки:

1. Ананченко, И.В., Информационная безопасность телекоммуникационных систем. Часть 1. Аппаратные ключи eToken. Средство защиты eToken Network Logon: учебное пособие / И.В Ананченко, П.И. Смирнов, Ю.М. Шапаренко. – СПб.: РГГМУ, – 2016. – 24 с., ил.

5.3. Промежуточный контроль: зачет, курсовая работа

Перечень вопросов для промежуточной аттестации (зачет):

1. Электронные ключи Guardant. Электронный ключ Guardant Sign. Электронный ключ Guardant Code. Лицензирование сетевых приложений. Защищенные схемы продаж.
2. Электронные ключи Guardant. Guardant SP. Сервер активации. Принцип работы. Технические характеристики.
3. Электронные ключи Guardant. Выбор модели ключа. Защита Windows-приложений.
4. Электронные ключи Guardant. Выбор модели ключа. Удаленное обновление памяти ключа. Guardant TRU API
5. Комплекты разработчика Guardant. Выбор модели ключа.
6. Электронный идентификатор Rutoken. Электронный идентификатор Rutoken. Комплект разработчика Rutoken
7. Комплект разработчика Rutoken. Электронные идентификаторы Рутокен Web.
8. Назначение ПО VipNet CUSTOM, VipNet OFFICE, ViPNet TUNNEL. Характеристики, общее и различие. ViPNet. Парольная защита. Файл дистрибутив (VipNet CUSTOM)
9. Состав программного комплекса ViPNet. Криптоядро Домен-К.
10. Логика обработки IP-трафика VipNet
11. Аппаратные ключи защиты серии HASP. Аппаратные ключи защиты HASP 4-го и 5-го поколения.
12. ViPNet Registration Point (Пункт Регистрации). Файл-дистрибутив VipNet. dst, КД и КН файлы.
13. Ключ Guardant: назначение, основные характеристики, пример использования
14. ViPNet Administrator (Администратор). Особенности ключевой структуры VipNet
15. Аппаратные ключи защиты RuToken
16. VipNet. Особенности взаимодействия ЦУС и УКЦ. Сетевые экраны: назначение, примеры использования.
17. Инфраструктура с открытыми ключами PKI. Аппаратные ключи защиты eToken
18. Виртуальные защищенные сети: виды, характеристики и варианты реализации.
19. Ключ eToken: назначение, основные характеристики, пример использования
20. Технология удостоверяющих центров VipNet. Режимы работы ViPNet Driver. Фильтрация, критерии и правила. Виды фильтров.
21. Ключ ruToken: назначение, основные характеристики, пример использования
22. Аппаратные ключи защиты серий HASP HL и HASP 4. Сравнительные характеристики, область применения.
23. Ключевой и удостоверяющий центр VipNet. Технология разграничения доступа к информации на примере ViPNet
24. Межсетевые экраны. ДМЗ. (на примерах VipNet). Создание виртуальной защищенной сети VipNet
25. Понятие адресной и прикладной администрации в ViPNet. Клиентское программное обеспечение для организации защищенной сети. ViPNet Client

(Клиент).

26. Логика использования виртуальных адресов в ViPNet. Компоненты ViPNet CUSTOM. ViPNet [Координатор]: назначение, особенности
27. VipNet. ЦУС и УКЦ, особенности взаимодействия. Криптоядро «Домен-К»
28. VipNet. Межсетевое взаимодействие. Виды ММК в VipNet. Серверное программное обеспечение для организации защищенной сети ViPNet Coordinator (Координатор)
29. VipNet. Ключи защиты, мастер ключи, ключи ЭЦП. Особенности ключевой структуры ViPNet. Этапы формирования ключевой информации.
30. Использование аппаратных ключей защиты eToken и HASP для защиты ПО и информации пользователей.
31. Методы, способы и средства защиты информации. Удостоверяющие центры ViPNet
32. Виды угроз безопасности в ТКС. Криптографические системы и их использование в VipNet.
33. ViPNet – сервер открытого Интернета. Транспортный модуль MFTP. Деловая почта. VPN как средство информационной защиты. Центры сертификации – назначение, техническая реализация.
34. Понятие – информационная безопасность. Информационная безопасность в сфере компьютерных сетевых технологий. Протокол https, криптопротоколы SSL, TLS.
35. Защита почтовых систем. Защита серверов и рабочих станций. Защита программного обеспечения – общие подходы и принципы. Электронные цифровые сертификаты. Принцип работы. Формальное описание. Структура сертификата. Российские стандарты.
36. Защита программного обеспечения с помощью аппаратных ключей серии Guardant
37. Семейство электронных ключей Guardant для защиты программного обеспечения от несанкционированного копирования и распространения.
38. Частные сети (VPN): принципы построения, конфигурирование, варианты реализации.
39. Защита программного обеспечения с помощью аппаратных ключей HASP HL, Hasp 4.
40. Ключи серий HASP HL и Hasp 4. Область применения, основные отличия.
41. Электронный ключ (аппаратный ключ). Принципы работы, классификация, примеры использования.
42. Хеш. Хеш-функция. Хеширование. Аутентификация, авторизация, идентификация.
43. Ключи серий ruToken и eToken – сравнительная характеристика, область применения.
44. Технологииаутентификации и шифрования. Реализация безопасной сетевой инфраструктуры для web-сервера.
45. История компьютерных вирусов. Классификация вирусов. Антивирусная защита компьютерной сети. Классификация антивирусов. Основные признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ.
46. Классификация firewall’ов и определение политики firewall’а
47. Обеспечение безопасности web-серверов. Безопасность web-содержимого. Электронные цифровые сертификаты; SSL/TLS
48. Защита ПО с помощью аппаратных или программных ключей Sentinel HASP

Образец карточки (билета) с вопросами зачета:

№ 1

1) Межсетевые экраны. ДМЗ. (на примерах VipNet). Создание виртуальной защищенной сети VipNet
2) Защита программного обеспечения с помощью аппаратных ключей серии Guardant.

Критерии оценивания.

Оценка «***отлично***» ставится студенту, ответ которого содержит:

- глубокое знание программного материала, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой;
- знание концептуально-понятийного аппарата всего курса; а также свидетельствует о способности:
- самостоятельно критически оценивать основные положения курса;
- увязывать теорию с практикой.

Оценка «***отлично***» не ставится в случаях систематических пропусков студентом семинарских и практических занятий по неуважительным причинам, а также неправильных ответов на дополнительные вопросы преподавателя.

Оценка «***хорошо***» ставится студенту, ответ которого свидетельствует о полном знании материала по программе, а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

Оценка «хорошо» не ставится в случаях систематических пропусков студентом семинарских и практических занятий по неуважительным причинам, а также неправильных ответов на дополнительные вопросы преподавателя.

Оценка «***удовлетворительно***» ставится студенту, ответ которого содержит:

- поверхностные знания важнейших разделов программы и содержания лекционного курса;
- затруднения с использованием научно-понятийного аппарата и терминологии курса;
- стремлениелогически четко построить ответ,а также свидетельствует о возможности последующего обучения.

Оценка «***неудовлетворительно***» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

Список примерных тем курсовых работ

1. Защита программного обеспечения программно-аппаратными ключами марки HASP HL Pro.
2. Защита программного обеспечения программно-аппаратными ключами марки HASP HL Basic.
3. Защита сетевого программного обеспечения программно-аппаратными ключами марки HASP HL Net

4. Лизинг программного обеспечения с использованием технологии защита программного обеспечения программно-аппаратными ключами марки HASP HL Time
5. Лизинг сетевого программного обеспечения с использованием технологии защита программного обеспечения программно-аппаратными ключами марки HASP HL TimeNet.
6. Обеспечение конфиденциальной работы с электронной почтой на основе электронных цифровых сертификатов, хранящихся в защищенных носителях аппаратных ключах серии e-token.
7. Обеспечение конфиденциальной работы с электронной почтой на основе электронных цифровых сертификатов, хранящихся в защищенных носителях аппаратных ключах серии ru-token.
8. Защита программного обеспечения комплекса, исполняемая программа формата ex4 и вызываемая ею библиотека dll, ключами серии HASP Hl.
9. Защита программного обеспечения комплекса, исполняемая программа формата ex4 и вызываемая ею библиотека dll, электронными ключами HASP Sl.
10. Защита программного обеспечения программно-аппаратными ключами марки SENTINEL
11. Реализация защищенного доступа к интернет-сайту с использованием аппаратного ключа Рутокен Web.
12. Развертывание VPN сетей, использование ключей серий eToken и ruToken для усиления защищённости VPN сети.
13. Использование электронной цифровой подписи при работе с электронными услугами.
14. Защита программного обеспечения с использованием программных ключей (HASP SL и GUARDANT SP).
15. Программы анализа хешей паролей. (C&A и др.)
16. Установка и настройка Центра сертификации, использование ключей eToken в домене Windows 2008R2/2012/2012R2/2016).
17.Сопровождение функционирования Центра сертификации, повышение защищенности систем на основе Windows 2008R2 (или Windows 2012/2012R2/2016).
18. Использование аппаратных токенов (eToken, ruToken) для работы с электронной цифровой подписью (ЭЦП).
19. Использование аппаратных токенов (eToken, ruToken) для защиты информации в базах данных (СУБД MS SQL Server и др.).
20. Инфраструктура открытых ключей PKI, взаимодействие с аппаратными токенами (eToken, ruToken).
21 Использование аппаратных токенов (eToken, ruToken) для защиты контента веб- серверов.
22. Использование аппаратных ключей для защиты электронных книг.
23 Использование аппаратных и программных ключей для защиты мультимедийного контента.
24 Использование электронных цифровых сертификатов, сохраненных в аппаратных ключах (eToken, ruToken) для аутентификации пользователей в операционных системах Windows (7/8/ Server 2008/

2008R2/2012/2012R2/2016).

25 Защита программного обеспечения (dll библиотек) с использованием аппаратного ключа SenseLock EL-Genii.

Критерии оценивания

Оценка «***отлично***» ставится студенту, ответ которого содержит:

- глубокое знание программного материала, а также основного содержания и новаций лекционного курса но сравнению с учебной литературой;
- знание концептуально-понятийного аппарата всего курса; а также свидетельствует о способности:
- самостоятельно критически оценивать основные положения курса;
- увязывать теорию с практикой.

Оценка «***отлично***» не ставится в случаях систематических пропусков студентом семинарских и практических занятий по неуважительным причинам, предоставление выполненной курсовой работы после установленной даты завершения выполнения курсовой работы, а также неправильных ответов на дополнительные вопросы преподавателя во время обсуждения выполненной курсовой работы.

Оценка «***хорошо***» ставится студенту, ответ которого свидетельствует о полном знании материала по программе, а также содержит в целом правильное, но не всегда точное и аргументированное изложение материала.

Оценка «***хорошо***» не ставится в случаях систематических пропусков студентом семинарских и практических занятий по неуважительным причинам, а также неправильных ответов на дополнительные вопросы преподавателя.

Оценка «***удовлетворительно***» ставится студенту, ответ которого содержит:

- поверхностные знания важнейших разделов программы и содержания лекционного курса;
- затруднения с использованием научно-понятийного аппарата и терминологии курса;
- стремление логически четко построить ответ, а также свидетельствует о возможности последующего обучения.

Выполненная курсовая работа ***не засчитывается*** и возвращается студенту на доработку, если существенные пробелы в знании основного материала по программе на закрепление которого была рассчитана курсовая работа, а также, если были допущены принципиальные ошибки при изложении материала.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Ананченко, И.В., Информационная безопасность телекоммуникационных систем. Часть 1. Аппаратные ключи eToken. Средство защиты eToken Network Logon: учебное пособие / И.В Ананченко, П.И. Смирнов, Ю.М. Шапаренко. – СПб.: РГГМУ, – 2016. – 24 с., ил. - Режим доступа: http://elib.rshu.ru/files_books/pdf/rid_934e2a15ca2e4a408df0517464e9941f.pdf

2. Проектирование защищенных информационных систем [Текст] : учебное пособие. Ч. 1. Конструкторское проектирование. Защита от физических

полей. . П. П. Бескид, В. Ю. Суходольский, Ю. М. Шапаренко. – СПб.: Изд-во РГГМУ, 2008. – 195 с. - Режим доступа: http://elib.rshu.ru/files_books/pdf/img-504175456.pdf
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2018. — 312 с. — (Серия : Специалист). — ISBN 978-5-9916-9043-0. — Режим доступа : www.biblio-online.ru/book/E458AFCD-826E-4A1F-9BAB-68BB83EA616F.
4. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — М. : Издательство Юрайт, 2018. — 342 с. — (Серия : Бакалавр и магистр. Модуль.). — ISBN 978-5-534-05142-1. — Режим доступа : www.biblio-online.ru/book/6A637EC7-8B78-4DA6-B404-71DE0202E2EF.

б) дополнительная литература:

1. Программно-аппаратные средства обеспечения информационной безопасности [Текст] : учебное пособие / А. В. Душкин [и др.] ; ред. А. В. Душкин. - Москва : Горячая линия -Телеком, 2017. - 247 с. - ISBN 978-5-9912-0470-5 : 619.00 р.

в) программное обеспечение и Интернет-ресурсы:

Программное обеспечение:

- windows 7
- office 2007
- dr Web
- Программа оптимизации структуры защищенной компьютерной сети с применением генетического алгоритма №2016611252
- Экспертная система выбора оптимальных средств защиты электронного контента №2016611251

Интернет-ресурсы

- https://biblio-online.ru – ЭБС Юрайт
- http://znanium.com – ЭБС Знаниум
- http://www.prospektnauki.ru – ЭБС Проспект науки
- http://elib.rshu.ru ЭБС ГидроМетеоОнлайн
- https://нэб.рф - Национальная электронная библиотека

7. Методические указания для обучающихся по освоению дисциплины (модуля)

Те	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

Практические	На практических занятиях выполняются задания по обеспечению информационной безопасности с использованием программно-аппаратных средств, изученных во время лекционных занятий. Как правило, на каждом занятии студент должен показать результаты выполнения практического задания преподавателю.
Внеаудиторная работа	представляет собой вид занятий, которые каждый студент организует и планирует самостоятельно. Самостоятельная работа студентов включает самостоятельное изучение разделов дисциплины.
Подготовка к зачёту	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

8. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Тема (раздел) дисциплины	Образовательные и информационные технологии	Перечень программного обеспечения и информационных справочных систем
Основы использования программно-аппаратных средств для обеспечения информационной безопасности.	Практическая	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Экспертная система выбора оптимальных средств защиты электронного контента Экспертная система выбора оптимальных средств защиты электронного контента Аппаратные ключи серий HASP, Guardant, eToken, ru-Token.
Идентификация пользователей КС – субъектов доступа к данным	Практическая	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Экспертная система выбора оптимальных средств защиты электронного контента Экспертная система выбора оптимальных средств защиты электронного контента Аппаратные ключи серий HASP, Guardant, eToken, ru-Token.

Средства и методы ограничения доступа к файлам	Практическая	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Экспертная система выбора оптимальных средств защиты электронного контента Экспертная система выбора оптимальных средств защиты электронного контента Аппаратные ключи серий HASP, Guardant, eToken, ru-Token.
Особенности защиты данных от изменения. Программно-аппаратные средства шифрования	Практическая	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Экспертная система выбора оптимальных средств защиты электронного контента Экспертная система выбора оптимальных средств защиты электронного контента Аппаратные ключи серий HASP, Guardant, eToken, ru-Token.
Построение программно-аппаратных комплексов шифрования	Практическая	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Экспертная система выбора оптимальных средств защиты электронного контента Экспертная система выбора оптимальных средств защиты электронного контента Аппаратные ключи серий HASP, Guardant, eToken, ru-Token.

Методы и средства ограничения доступа к компонентам ЭВМ	Практическая	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Экспертная система выбора оптимальных средств защиты электронного контента Экспертная система выбора оптимальных средств защиты электронного контента Аппаратные ключи серий HASP, Guardant, eToken, ru-Token.
Особенности защиты данных от изменения. Программно-аппаратные средства шифрования	Практическая	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Экспертная система выбора оптимальных средств защиты электронного контента Экспертная система выбора оптимальных средств защиты электронного контента Аппаратные ключи серий HASP, Guardant, eToken, ru-Token.
Защита программ от изучения. Аппаратный ключ с точки зрения электроники.	Практическая	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Экспертная система выбора оптимальных средств защиты электронного контента Экспертная система выбора оптимальных средств защиты электронного контента Аппаратные ключи серий HASP, Guardant, eToken, ru-Token.

Защита от разрушающих программных воздействий.	Практическая	https://biblio-online.ru http://znanium.com http://www.prospektnauki.ru http://elib.rshu.ru https://нэб.рф windows 7 office 2007 dr Web Экспертная система выбора оптимальных средств защиты электронного контента Экспертная система выбора оптимальных средств защиты электронного контента Аппаратные ключи серий HASP, Guardant, eToken, ru-Token.

9. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

При определении формы проведения занятий с обучающимся-инвалидом учитываются рекомендации, содержащиеся в индивидуальной программе реабилитации инвалида, относительно рекомендованных условий и видов труда.

При необходимости для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья создаются специальные рабочие места с учетом нарушенных функций и ограничений жизнедеятельности.

10. Материально-техническое обеспечение дисциплины

Учебная аудитории для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).

Учебная аудитория для групповых и индивидуальных консультаций - укомплектована специализированной (учебной) мебелью, техническими средствами обучения, служащими для представления учебной информации.

Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечено доступом в электронную информационно-образовательную среду организации

Помещение для хранения и профилактического обслуживания учебного оборудования – укомплектовано специализированной мебелью для хранения оборудования и техническими средствами для его обслуживания.

Лаборатория - Лаборатория Программно-аппаратных средств обеспечения информационной безопасности. Помещение оснащено: специализированной (учебной) мебелью, 15 компьютеров, антивирусными программными комплексами и аппаратными средствами аутентификации пользователя

Для эффективной работы в рамках дисциплины рекомендуется иметь возможность работать с пакетами специализированных программ, сохраненными на съемных накопителях информации.

Для выполнения лабораторных работ используется специализированное аппаратное обеспечение:

Стартовый комплект SDK Sentinel HASP Pro;
Стартовый комплект SDK Sentinel HASP Time; Стартовый комплект SDK Sentinel HASP Net; Стартовый комплект SDK Sentinel NetTime; Стартовый комплект SDK Sentinel HASP Drive.
Аппаратные ключи серий HASP, Guardant, eToken, ruToken.

Рассмотрено и рекомендовано к использованию в учебном процессе на 2019/2020 учебный год с изменениями (смотри лист изменений)

Протокол заседания кафедры ИТиСБ от 07.05.2019 №5

Лист Изменений

Изменения, внесенные протоколом заседания кафедры ИТиСБ от 07.05.2019 №5

1. Дисциплина перенесена на 7 семестр.